

Державний вищий навчальний заклад
Донецький національний технічний університет
Кафедра прикладної математики та інформатики

«ЗАТВЕРДЖУЮ»

Перший проректор

_____ Леонід БАЧУРІН

«_____» _____ 2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОНД 2.11 МАТЕМАТИЧНІ МЕТОДИ КРИПТОГРАФІЇ

(шифр і назва навчальної дисципліни)

Рівень освіти: перший (бакалаврський)

Спеціальність

125 Кібербезпека

(шифр і назва спеціальності (тей))

Освітня програма

Кібербезпека

(назва освітньої програми)

Мова навчання: українська

Робоча програма навчальної дисципліни «Математичні методи криптографії»
(повна назва дисципліни)

для здобувачів вищої освіти за спеціальністю 125 Кібербезпека «30» 08 2023 року. – 8 с.

Розробник:

Людмила КОВАЛЬЧУК, д.т.н., проф., професор кафедри ПМІ

Робоча програма затверджена на засіданні кафедри прикладної математики та інформатики

Протокол № 8 від “31” серпня 2023 р.

Завідувач кафедри прикладної математики та інформатики

_____ (Наталія МАСЛОВА)

“31” серпня 2023 р.

Схвалено науково-методичною комісією галузі знань 12 Інформаційні технології

Протокол № 5 від “ 1” 09 2023р.

Голова _____ (Євген БАШКОВ)
(підпис) (прізвище та ініціали)

1. Загальна інформація

Форма навчання	Денна
Статус	Обов'язкова
Обсяг в кредитах ЄКТС	6
Обсяг в годинах за навчальним планом, разом:	180
в тому числі:	
лекції:	32
практичні заняття:	32
самостійна робота:	116
Розрахункова робота	
Форма підсумкового контролю	Екзамен
Дисципліну викладають	Викладач проф. Ковальчук Л.В., lyudmila.kovalchuk@donntu.edu.ua lyudmila.kovalchuk@iohk.io lyudmila_kovalchuk@adoriasoft.com

Передумови для вивчення дисципліни: перелік дисциплін, які мають бути вивчені раніше: Вища математика, Програмування, Теорія ймовірностей та математична статистика, Основи інформаційної безпеки, Методи та засоби криптографічного захисту інформації, Інформаційно-комунікаційні системи, Захист операційних систем.

2. Мета вивчення навчальної дисципліни

Метою вивчення навчальної дисципліни є опанування методами та засобами технічного захисту інформації, підготовка фахівців, здатних розробляти і використовувати технології інформаційної та/або кібербезпеки.

Загальні компетентності:

- ІК. Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної та/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
- ЗК 1. Здатність застосовувати знання у практичних ситуаціях.
- ЗК.2. Знання та розуміння предметної області та розуміння професії.
- ФК 2. Здатність до використання інформаційно- комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.
- ФК 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах
- ФК 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.

Програмні результати навчання:

ПРН4. аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення

ПРН6. критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

ПРН19. застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах

ПРН47. вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації

ПРН48. виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах

3. Очікувані результати навчання

Результатами навчання є оволодіння практичними навичками з проведення процедур криптографічного захисту інформації, застосування криптографічних протоколів, застосування концептуальних знань з навчальних дисциплін загальної підготовки для засвоєння дисциплін професійної підготовки.

В цілому результатами вивчення даної дисципліни є оволодіння математичним апаратом, що використовується у криптографічному захисті інформації, підготовка фахівців, здатних розробляти і використовувати технології інформаційної та/або кібербезпеки.

4. Засоби діагностики результатів навчання

Поточний контроль здійснюється під час проведення практичних занять і має на меті перевірку рівня підготовленості студента до виконання конкретної роботи. Форма проведення поточного контролю – усна бесіда за результатами виконання практичних робіт.

Підсумковий контроль проводиться з метою оцінювання результатів навчання та визначається підсумками результатів виконання та захисту практичних робіт по кожній зі змістовних тем.

Підсумковий семестровий контроль – іспит.

5. Критерії оцінювання результатів навчання

Критерії оцінювання мають формувати порядок оцінювання під час поточного контролю (за результатами практичних, лабораторних, семінарських занять та виконання індивідуальних або групових завдань) та підсумкового контролю.

ПР 1	ПР 2	ПР 3	ПР 4	ПР 5	ПР 6	ПР 7	ПР 8	ІНДЗ	Поточний контроль	Екзамен	Максимальний бал
4	4	4	4	4	4	4	4	8	40	60	100
2	2	2	2	2	2	2	2	8	24		84

Примітка: 1) Пр1, Пр2 і т.д практичні роботи;

Сз1, Сз2 і т.д семінарські заняття;

2) У числівнику максимальний бал – при своєчасному та правильному виконанні, у знаменнику – мінімальний (при правильному, але несвоєчасному виконанні)

В оцінку поточного контролю з виконання лабораторних робіт включено контрольні та поточні опитування

Результати підсумкового контролю оцінюються за 100-бальною шкалою та чотирибальною («відмінно», «добре», «задовільно», «незадовільно»).

Відповідність між шкалами встановлюється наступним чином:

Оцінка	
За 100-бальною шкалою	Для екзамену
90-100	відмінно
74-89	добре
60-73	задовільно
0-59	незадовільно

6. Програма навчальної дисципліни

6.1. Основні теми дисципліни

Тема 1. Основи абстрактної алгебри.

Лекція 1/1. Вступна Лекція. Системи числення. Модулярна арифметика.

Лекція 1/2. Алгебраїчні системи з однією операцією. Приклади, властивості. Означення підгрупи та класів суміжності. Властивості класів суміжності. Порядок елемента групи.

Лекція 1/3. Теорема Лагранжа, наслідки. Означення та властивості циклічної групи. Група перестановок.

Лекція 1/4. Відображення груп: гомоморфізм, ізоморфізм. Властивості відображень груп. Ядро та образ гомоморфізму.

Лекція 1/5. Алгебраїчні системи з двома операціями. Відображення.

Лекція 1/6. Мультиплікативна група кільця з одиницею. Характеристика кільця, характеристика поля.

Тема 2. Основи теорії чисел.

Лекція 2/1. Означення часу роботи алгоритмів. Час роботи арифметичних операцій. Схема Горнера піднесення до степеню. Імовірнісні алгоритми. Лас-Вегас та Монте-Карло алгоритми. Алгоритми розпізнавання мови з однією помилкою.

Лекція 2/2. Прості та складені числа. Ділення з остачею. НСД та НСК. Алгоритм Евкліда обчислення НСД. Наслідки алгоритму Евкліда. Мультиплікативна група кільця лишків.

Лекція 2/3. Означення конгруенції. Властивості конгруенцій. Розв'язок конгруенцій.

Лекція 2/4. Системи конгруенцій. Китайська теорема про лишки (проста та узагальнена). Розв'язок системи конгруенцій.

Лекція 2/5. Мультиплікативна група скінченного поля. Алгоритм пошуку примітивних елементів поля. Квадратичні лишки та нелишки. Властивості квадратичних лишків. Псевдопрості числа. Числа Кармайкла. Генерація простих чисел.

Лекція 2/6. Однобічні функції та складнорозв'язувані задачі. Приклади. Використання однобічних функцій для побудови класичних асиметричних криптосистем.

Тема 3. Скінченні поля.

Лекція 3/1. Означення та властивості кільця поліномів. Незвідні поліноми.

Лекція 3/2. Основна характеристична теорема скінченних полів. Побудова скінченного поля. Означення підполя, критерій підполя.

Лекція 3/3. Означення еліптичної кривої. Побудова еліптичних кривих над скінченними полями.

Лекція 3/4. Найпростіші криптосистеми на еліптичних кривих.

6.2. Теми лабораторних (семінарських) занять

Проведення лабораторних занять не передбачено навчальним планом дисципліни

6.3. Теми практичних робіт

№ з/п	Назва теми	Кількість годин
1	Практична робота №1. Розв'язок задач на системи числення та модулярну арифметику.	4
2	Практична робота №2. Алгебраїчні системи з однією операцією. Здобуття навичок роботи з групами.	4
3	Практична робота №3. Алгебраїчні системи з двома операціями.	2
4	Практична робота №4. Мультиплікативні групи. Характеристики кільця й поля.	4
5	Контрольна робота за Лекціями 1-6	2
6	Практична робота №5. Імовірнісні алгоритми й визначення часу роботи алгоритмів. Виконання обчислень з використанням схеми Горнера та узагальненої теореми Ойлера.	4
7	Практична робота №6. Прості та складені числа. Розв'язування конгруенцій та систем конгруенцій.	4
8	Практична робота №7. Визначення квадратичних лишків, розв'язування квадратних рівнянь у скінченних кільцях.	4
9	Практична робота №8. Побудова асиметричних криптосистем у простих полях.	2
10	Контрольна робота за темами 2-3	2
...	Усього годин	32

6.4. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Системи числення. Модулярна арифметика.	8
2	Алгебраїчні системи з однією операцією.	8
3	Теорема Лагранжа, наслідки.	6
4	Відображення груп: гомоморфізм, ізоморфізм.	6
5	Алгебраїчні системи з двома операціями. Відображення.	8
6	Мультиплікативна група кільця з одиницею.	8
7	Означення часу роботи алгоритмів.	8
8	Прості та складені числа. Алгоритм Евкліда.	6
9	Властивості конгруенцій.	6
10	Системи конгруенцій. Розв'язок системи конгруенцій.	8
11	Мультиплікативна група скінченного поля. Алгоритм пошуку примітивних елементів поля.	8
12	Однобічні функції та складнорозв'язувані задачі.	8
13	Властивості кільця поліномів.	6
14	Побудова скінченного поля.	6
15	Побудова еліптичних кривих над скінченними полями.	8
16	Криптосистеми на еліптичних кривих.	8
...	Усього годин	116

6.5. Індивідуальні та/або групові завдання

Студенти виконують індивідуальне завдання з дисципліни. Тематика роботи: «Скінченні поля».

7. Література

7.1. Основна

1. Ковальчук Л.В., Яремчук Ю.Є. Прикладна алгебра. Частина 1. Основи абстрактної алгебри : навчальний посібник / Л.В. Ковальчук, Ю.Є. Яремчук. – Вінниця : ВНТУ, 2015. – 99 с.
2. Л. Ковальчук, С. Конюшок, Н. Кучинська. Прикладна алгебра: основні поняття алгебри та теорії чисел. Навчальний посібник. 2010. 181 стор.
3. Л. Ковальчук., А. Кудін, Н. Кучинська. Математичні аспекти теорії блокчейн. Навчальний посібник. 2022. 141с.
4. ДСТУ 9041:2020 Алгоритм шифрування коротких повідомлень.
5. Justin Thaler. Proofs, Arguments, and Zero-Knowledge. June 27, 2022. 320p.
6. William J. Buchanan, Shancang Li & Rameez Asif. Lightweight cryptography methods. Journal of Cyber Security Technology. Volume 1, 2017 - Issue 3-405 Mar 2018. Pages 187-201.
7. Masanobu Katagi and Shiho Moriai. Lightweight Cryptography for the Internet of Things.

7.2 Допоміжна

8. A. Bogdanov¹, L.R. Knudsen², G. Leander¹, C. Paar¹, A. Poschmann¹, M.J.B. Robshaw³, Y. Seurin³, and C. VIKKELSOE. PRESENT: An Ultra-Lightweight Block Cipher. 2007. 18p.
9. Вербицький О. В. Вступ до криптології / О.В. Вербицький– Львів: Видавництво науково-технічної літератури, 1998. – 247 с.
10. Koblitz N. Number theory and cryptology. / Cambridge, 1993, 254 p.
11. Leon Groot Bruinderink. Towards Post-Quantum Bitcoin. A thesis submitted in partial fulfillment of the requirements for the degree of Master of Science in Industrial and Applied Mathematics. 2016. 81p.
12. Kerry A. McKay, Larry Bassham, Meltem Sönmez, Turan Nicky Mouha. NISTIR 8114 Report on Lightweight Cryptography. 2017. 27p.
13. Maksym Petkus. Why and How zk-SNARK Works: Definitive Explanation. 2019. 65p.
14. Харин Ю.С. Математичні комп'ютерні основи криптології: Навч. посібник / Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Агеевич.: Нове знання, 2003. – 382 с.
15. Гапак О.М. Навчальний посібник Криптоаналіз. Криптографічні протоколи. Ужгород, 2021. 82с.

7.3. Методична

Методичні вказівки до виконання практичних робіт з дисципліни «Математичні методи криптографії» для студентів денної форми навчання ОС «бакалавр» спеціальності 125 Кібербезпека (планується до видання).

8. Інформаційні ресурси

1. Гапак О.М. Посібник з курсу «Комп'ютерна криптографія» <https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/36505/1/Криптоаналіз.%20Криптографічні%20протоколи.pdf>
2. Криптографічні протоколи, <http://um.co.ua/8/8-2/8-241181.html>